Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 28 June 2005

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- The Associated Press reports an American Airlines flight that had taken off on a flight to Rome returned to O'Hare International Airport because a passenger found a small knife inside an airline−provided package containing a pillow and blanket. (See item 3)
- The Macon Telegraph reports invasive species are an increasing danger, a leading cause of extinctions and crop damage, and now even considered a potential form of bioterrorism. (See item 7)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS/IAIP Products &Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *June 27, Associated Press* — **Fire extinguished at nuclear plant.** A fire at the Turkey Point nuclear power plant was extinguished Monday, June 27, with no damage to the plant's two nuclear units, according to Florida Power and Light (FPL). The blaze started about 3:15 a.m. in a transformer in the plant's number four unit, an area that was not near the nuclear facilities, FPL spokesperson Bill Swank said. The company's power customers were not affected. The affected unit was taken offline while the cause of the fire was investigated. Swank said the extent of damage was not yet known. Turkey Point is located on Biscayne Bay, 24 miles south of Miami, FL.
Source: http://www.sun−sentinel.com/news/local/miami/sfl−627turkey,0

,3444841.story?coll=sfla−news−miami

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

2. *June 26, Associated Press* — **University discovers server breach.** The University of Connecticut is notifying 72,000 students, staff, and faculty as a precaution after officials found a computer−hacking program in a server at the school. The server contains names, Social Security numbers, dates of birth, phone numbers, and addresses for anyone with an account that allows access to the school's computer network. The personal information was not in a readable format, officials said. University officials found the computer−hacking program this week and said it had been placed in a server at the school in 2003. The security breach was discovered on Monday, June 20, after a university vendor reported that someone tried to access its server with an illegal password. Technology staff discovered that a program known as a rootkit had been installed on the server. The server was immediately taken offline, chief information officer Michael Kerntke said.
   Source: http://www.informationweek.com/showArticle.jhtml?articleID=1 64902812

[Return to top]

Transportation and Border Security Sector

3. *June 27, Associated Press* — **Plane with knife on board turns around, returns to Chicago.** An American Airlines flight that had taken off on a flight to Rome returned to O'Hare International Airport in Chicago, IL, because a passenger found a small knife on board, an airline spokesperson said Sunday, June 26. American Airlines Flight 110 had been in the air for more than an hour Saturday, June 25, when the passenger found the knife inside an airline−provided package containing a pillow and blanket, American spokesperson Mary Frances Fagan said. The plane returned to O'Hare as a security precaution, Fagan said. The Boeing 767−300 had 199 passengers. Fagan said the airline did not know how the knife got into the plastic−wrapped package. Airline personnel found nothing suspicious on board following the landing.
   Source: http://www.usatoday.com/news/nation/2005−06−26−knife−on−plan e_x.htm

4. *June 27, Canadian Press* — **Passenger boards Canadian flight without proper screening.** Thousands of passengers and more than 50 flights were delayed at British Columbia's Vancouver airport on Sunday, June 26, when a man bypassed security screening and flew to his destination without being detected. "Any such incident calls into question safety and security," said Jacqueline Bannister of the Canadian Air Transportation Security Authority, which is investigating. "The guy went through pre−board screening at Vancouver without getting properly screened and he got on his plane and the plane left Vancouver with him on it and he arrived in Toronto. Nobody knew that he was actually on the flight [to] Toronto." Bannister was unable to explain the double−security breach: the man getting past pre−board screening and then getting on the flight that was able to take off even though he hadn't been screened. About 3,000 people in the departure areas, and passengers already on board up to six flights, were ordered back into the terminal to be screened again. The passenger was eventually identified during re−screening in Toronto. It does not appear the man had any criminal intent but there will be a "full post−mortem" on how he was able to bypass security and get on a plane, Bannister said.
   Source: http://www.canada.com/vancouver/story.html?id=ae9e5237−ac45−416e−aee9−6e1d47e9df3c

5. *June 27, Globe and Mail (Canada)* — **Maker of Amtrak brakes switched designs.** The supplier of the brakes that paralyzed Amtrak's high−speed Acela trains after developing potentially catastrophic cracks changed the design of the parts while the trains were being built to include longer, thinner spokes that might have been weaker than the original design. Investigations by Amtrak, the U.S. government, and companies that helped manufacture the Acela haven't yet concluded there is any link between the revised brake design and cracks discovered in April in hundreds of the 1,440 brake discs used to stop the trains. But scrutiny has fallen on the change, and the plan for getting the trains rolling again as soon as next month includes installing brakes based on the abandoned design. The decision to replace the original design and now revive it to get Acela trains back on track raises new questions about Amtrak's handling of the Acela project, which has been hobbled by problems almost from the start.
   Source: http://www.theglobeandmail.com/servlet/ArticleNews/TPStory/LAC/20050627/RAMTRAK27/TPInternational/Americas

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

6. *June 27, United Press International* — **Bird flu detected in Japan.** A diluted strain of bird flu virus has been turned up at a poultry farm in Mitsukaido, Ibaraki Prefecture, the first time the strain has been confirmed in Japan. Unlike the avian flu virus that last year infected farms in Yamaguchi and Kyoto prefectures, the strain is not especially virulent, and only a small percentage of the infected chickens have died, according to officials from the agriculture

ministry and the Ibaraki prefectural government, the Asahi Shimbun reported Monday, June 27. Japan's government Monday began the extermination of about 25,300 chickens at the farm to kill the influenza virus.
Source: http://washingtontimes.com/upi/20050627−065611−6139r.htm

7. *June 26, Macon Telegraph (GA)* — **Invasive species are an increasing danger.** Wildlife as a form of pollution is a relatively new concept, but one the federal government has come to emphasize in the past 10 years. That's because invasive species are a leading cause of extinctions and crop damage, and now they're even considered a potential form of bioterrorism. Invasive species are plants or animals from another part of the state or world that grow out of control when introduced into a new habitat, often damaging the environment and crowding out native species. They kill everything in Georgia from oak trees to soybeans to bald eagles. "Once these things get established, they're almost impossible to get rid of. In that sense, it's one of the worst forms of pollution, because it can't be undone," said Brett Albanese, aquatic zoologist for the state Department of Natural Resources. Invasive species move around the world as never before through international trade −− some brought deliberately, others as hitchhikers. Georgia is especially susceptible as home to Hartsfield−Jackson Atlanta International Airport and Savannah's port, the sixth largest in the nation. Dozens of species threaten state and national park land, according to a study by the Georgia Green Industry Association exotic pest plant task force.
Source: http://www.macon.com/mld/macon/11978200.htm

8. *June 24, Reuters* — **European Union ministers uphold sovereign right to ban genetically modified crops.** European Union (EU) environment ministers dealt a blow on Friday, June 24, to efforts to get more genetically modified (GM) crops grown in Europe as they agreed to uphold eight national bans on GM maize and rapeseed types. The vote was a sharp rebuff for the European Union's executive Commission, which had wanted the ministers to endorse an order to lift the bans within 20 days. EU law provides for national GM bans if the government can justify the prohibition. The U.S., Canada, and Argentina have sued the EU at the World Trade Organization (WTO) alleging that EU biotech policy harms trade and is not founded on science. The EU's 1998−2004 biotech ban, they say, was illegal. The WTO is now expected to issue its initial ruling on the GM case in early October, postponed from August, officials say.
Source: http://today.reuters.co.uk/news/newsArticle.aspx?type=worldNews&storyID=2005−06−24T154755Z_01_EIC441989_RTRUKOC_0_FOOD−E U−GMO.xml

9. *June 21, U.S. Department of Agriculture* — **Funds awarded to states and tribes for animal identification premises registration.** U.S. Department of Agriculture (USDA) Secretary Mike Johanns Tuesday, June 21, announced that USDA will be accepting funding applications from state and tribal governments to continue registering premises for the national animal identification system (NAIS). Approximately $14.3 million will be available to state and tribal cooperators. "Identifying farms and ranches where animals are held is a first step in establishing our national animal identification system," said Johanns. "More than 80,000 premises have been registered so far and that momentum is building." Currently, animal health officials conduct disease trace outs with systems already in place, such as records related to program diseases, on−farm recordkeeping, required interstate movement certificates and breed registries. However, these epidemiologic investigations may take days to weeks to complete because records are often kept on paper or because they are not standardized across state lines. In 2004,

the USDA's Animal and Plant Health Inspection Service (APHIS) and its state, tribal and industry partners began implementing a national system that will help trace diseased or potentially diseased animals to their point of origin more quickly and efficiently. Identifying premises is the first step toward creating the tracking system. Currently, 47 states and five tribes have approved premises registration systems, and APHIS anticipates that all 50 states will be on board by July 2005.
Source: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB?contentidonly=true&contentid=2005/06/0223.xml

[Return to top]

Food Sector

10. *June 27, Associated Press* — **Japan: U.S. mad cow case won't affect ban.** Japan's top government spokesperson, Chief Cabinet Secretary Hiroyuki Hosoda, said Monday, June 27, that the latest confirmed U.S. case of mad cow disease will not affect deliberations on ending a 17−month ban on American beef imports. Japan was the United States' largest overseas market for beef before Tokyo banned all U.S. beef imports following the first confirmed U.S. mad cow case in December 2003. The confirmation by the U.S. Department of Agriculture Friday, June 24, followed a series of conflicting results that prompted Japanese experts to question the accuracy of the U.S. testing procedures. Japan and the U.S. struck a deal last fall to resume limited imports of cows younger than 21 months considered less at risk of the disease, but those plans were delayed by a dispute on testing standards used to determine the age of cattle. Japan's Food Safety Commission took a key step last month by recommending the government end its domestic policy of blanket testing all cows headed for market. Such an easing would likely allow imports of U.S. beef from cattle younger than 21 months to also resume.
Source: http://seattlepi.nwsource.com/national/apscience_story.asp?category=1500&slug=Japan%20US%20Mad%20Cow

11. *June 26, Food Safety and Inspection Service* — **Sausage recalled.** Los Galleguito, a Union City, NJ, firm, is voluntarily recalling approximately 720 pounds of Spanish sausage that may be contaminated with Listeria monocytogenes, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Sunday, June 26. The sausages were distributed through retail stores in Florida. The problem was discovered through routine FSIS microbial sampling. FSIS has received no reports of illnesses associated with consumption of these products. Consumption of food contaminated with Listeria monocytogenes can cause listeriosis, an uncommon but potentially fatal disease.
Source: http://www.fsis.usda.gov/News_&_Events/Recall_029_2005_Relea se/index.asp

[Return to top]

Water Sector

12. *June 27, Associated Press* — **Governor activates task force to deal with drought.** Illinois Governor Rod Blagojevich has activated the Drought Response Task Force following one of the driest springs on record. The National Weather Service says most of Illinois is at moderate

risk for drought, but the drought risk is severe for the North Central part of the state. The Drought Response Task Force is made up of experts from several state agencies. They will monitor community water supplies and watch how the drought affects wildlife and natural areas. The impact on corn and soybean crops also will be watched closely.
Source: http://abclocal.go.com/wls/news/062705_ap_ns_drought.html

[Return to top]

Public Health Sector

13. *June 27, China Daily* — **Two died as plague reported in Tibet.** Two persons died of bubonic plague and three others are recovering from the disease in the Tibet Autonomous Region in southwest China, the regional government's information office reported on Saturday, June 25. The outbreak occurred in Zhongba, a county in Xigaze Prefecture bordering Nepal, and has been brought under control, the office said. The Ministry of Health reported the infections to the World Health Organization and Nepal early Saturday morning. The disease was discovered when nine people who had come to Zhongba from Mianyang City in southwest China's Sichuan Province ate marmot meat on June 11; five of them later felt sick. Tibet's public health department dispatched a ten−member task force to deal with the situation when it received a report on the infections on June 17. The work team traced 76 direct contacts; 75 of them are now under quarantine and show no abnormal symptoms. The other one went to Nepal, and police are now searching for her. The quarantine will continue for another 15 days.
Source: http://www.chinadaily.com.cn/english/doc/2005−06/27/content_454975.htm

14. *June 27, National Institutes of Health* — **Cancer drug slows pox virus in mice.** Mice given a relatively new cancer drug can survive an otherwise lethal dose of vaccinia virus, a relative of smallpox virus, report scientists supported by the National Institute of Allergy and Infectious Diseases (NIAID), part of the National Institutes of Health. The findings, say the investigators, suggest that Gleevec or similar drugs might be useful in preventing adverse side effects of smallpox vaccine. Like all viruses, poxviruses co−opt various cellular molecules and processes to enter a cell, replicate, and then spread to uninfected cells. To learn whether Gleevec could prevent or lessen vaccinia's ability to spread in a living organism, the researchers treated mice with either saline solution or with Gleevec at a dose equivalent to that given to humans being treated for chronic myelogenous leukemia (CML). Next, they exposed the mice to ordinarily lethal amounts of vaccinia. All of the Gleevec−treated mice survived, while 70 percent of the untreated mice died. This finding suggests that Gleevec might play a role in addressing a public health emergency in the event of a smallpox outbreak. Administered for a short period, Gleevec theoretically could hamper the cell−to−cell spread of virus and allow the body's immune system to mount a successful defense.
Source: http://www.nih.gov/news/pr/jun2005/niaid−27.htm

15. *June 24, Associated Press* — **Group estimates potential flu death toll.** More than a half−million people could die and more than 2.3 million could be hospitalized if a moderately severe strain of pandemic flu virus hits the United States, a research group said Friday, June 24. The report from the Trust for America's Health (TFAH) assumes that 25 percent of a country's population would become infected if a strain of avian flu became highly contagious and humans had no natural immunity against it. The researchers also assumed the severity of the

strain would fall about midway between the pandemic of 1918 and the pandemic of 1968. The research group says the staggering number of potential deaths and hospitalizations would overwhelm the nation's health care system and displays the need for greater planning and resources. The Trust for America's Health called on lawmakers to provide more than the $58 million that they've already approved for purchasing influenza countermeasures, specifically Tamiflu, for a national stockpile. The group estimated that the federal government has ordered 5.3 million courses of Tamiflu for the stockpile, but that it would require about 70 million doses to cover 25 percent of the U.S. population, which is the rate the World Health Organization has recommended.
TFAH report: http://healthyamericans.org/reports/flu/Flu2005.pdf
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/06/24/AR2005062401368.html

16. *June 24, Agence France Presse* — **WHO boosting Angola's ability to tackle Marburg on its own.** The World Health Organization (WHO) said that it was aiming to ensure that Angolan health authorities could tackle a deadly epidemic of Marburg haemorrhagic fever without international help. Iain Simpson, spokesperson for the United Nations health agency, said international experts have been helping Angolan counterparts build up laboratory capacity and other medical services. The death toll from the Ebola−like fever in Angola has climbed past 350 since it broke out last October, with the outbreak centered in the country's northern Uige province. There have been no reported new cases since June 12, said Simpson. However, the outbreak cannot be declared officially over until 42 days, or twice Marburg's incubation period−have elapsed without new cases, he noted. There is no cure for the virus, whose exact origin is unknown and which was first detected in 1967 when West German laboratory workers in the town of Marburg were infected by monkeys from Uganda. It spreads through contact with bodily fluids such as blood, excrement, vomit, saliva, sweat and tears but can be contained with relatively simple hygienic precautions, according to experts.
Source: http://news.yahoo.com/s/afp/20050624/hl_afp/whoangolahealthvirus_050624142425;_ylt=AjGZTFw8Y_RZMuDk9.yFemeJOrgF;_ylu=X3oDMTBiMW04NW9mBHNlYwMlJVRPUCUl

[Return to top]

Government Sector

17. *June 27, Department of Homeland Security* — **United States, Mexico, and Canada deliver initial Security and Prosperity Partnership report.** Department of Homeland Security Secretary Michael Chertoff and Department of Commerce Secretary Carlos Gutierrez and their government counterparts in Mexico and Canada released on Monday, June 27, the first report of the Security and Prosperity Partnership of North America that identifies initial results, key themes and initiatives, and work plans that further promote the security and prosperity of North America. Among the security goals identified in the report, all three countries have agreed to establish a single, integrated North American Trusted Traveler Program in less than three years. This program will offer a single application portal and enrolled participants will have access to all trusted traveler dedicated lanes at land, air and sea ports of entry.
Department of Homeland Security Fact Sheet:
http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0695.xml

For more information on the Security and Prosperity Partnership of North America, visit http://www.spp.gov.
Source: http://www.dhs.gov/dhspublic/display?content=4552

[Return to top]

Emergency Services Sector

18. *June 27, The Journal News* — **Emergency drill works on shooting, gas attack.** The White Plains and Westchester County Hazardous Materials Response Teams in New York were called to White Plains High School on Sunday, June 26, for a possible biochemical release that would later prove to be the highly toxic sarin gas. As the Hazmat team suited up in "Level A" gear, four men, coughing and gasping for air, exited the building and fell to the ground. They were transported to the decontamination area where they were hosed down with water and bleach. The simulated terrorist−attack response was put on by the White Plains Department of Public Safety, in cooperation with the Westchester County Office of Emergency Personnel and several county and local public safety agencies yesterday morning at the high school. "The importance of this drill is to bring multiple jurisdictions together to see how we do," said Public Safety Commissioner Frank Straub. "We're all working under what's called 'unified incidence command.' " Observers were on hand, positioned around the school, evaluating the response efforts. Detailed reports on the participants' performance would be sent to the state and federal level in the coming weeks, said Martin Gleeson, spokesperson for the Department of Public Safety.
Source: http://www.thejournalnews.com/apps/pbcs.dll/article?AID=/20050627/NEWS02/506270316/1018

19. *June 26, Reno Gazette−Journal (NV)* — **Nevada county plans massive terror drill.** With a $400,000 federal grant to pay extra wages for firefighters, police and other first responders, Washoe County is organizing a full−scale training exercise for November involving a terrorist plot and hazardous materials. Aaron Kenneston, county emergency operations manager, said several hundred people will take part. Sparks officials will lead the practice drill involving pretend terrorists and first responders wearing chemical−protection suits, he said. Creating the exact plot will be part of the exercise. Reno officials oversaw a training exercise in late May at the Reno/Tahoe International Airport. In that exercise, county deputies took to casino rooftops to look for pretend terrorists who shot down an aircraft with a shoulder−fired missile launcher. The county oversaw a flood−alert exercise earlier in the year. About 20 to 30 responders will begin with a weeklong training program on how to conduct a training exercise to meet Homeland Security standards, go through several tabletop exercises and then put together the regional exercise. They'll conduct exercises, drills and keep refining the exercise in monthly progress reviews.
Source: http://www.rgj.com/news/stories/html/2005/06/26/102692.php?sps=rgj.com&sch=LocalNews&sp1=rgj&sp2=News&sp3=Local+News&sp5=RGJ.com&sp6=news&sp7=local_news&jsmultitag=news.rgj.com/new s/local

20. *June 25, Curry Coastal Pilot (OR)* — **Officials in southern Oregon approve new tsunami warning plan.** The next time there is a tsunami warning for the southern coast of Oregon, both fire stations in both Brookings and Harbor will air their sirens simultaneously. Emergency

officials using the 911 dispatch center in Brookings agreed to the plan Thursday, June 23, following the confusion of the June 14 earthquake and tsunami warning during which neither fire station sounded a warning siren. A new electronic method of activating both fire station sirens will be installed within six months, Brookings Police Lt. John Bishop said. The button will be triggered only when the official word comes from the National Warning System (NAWAS.)
Source: http://www.currypilot.com/news/story.cfm?story_no=10982

21. *June 24, County of Rockland (NY)* — **Disaster exercise to highlight emergency response.** On Wednesday, June 29, the Rockland Emergency Services Combined Unit Exercise, "RESCUE 2005," will take place on the campus of the Rockland Community College in Suffern, NY. The Rockland County Office of Fire and Emergency Services in partnership with the Rockland County Sheriff's Department, the Rockland Regional Entry and Counterterrorism Team (REACT), the County Department of Health, the Town of Ramapo Police Department and Rockland Community College personnel have developed a scenario to test the response capabilities of local and County emergency response personnel in the event of a mass casualty incident. Participants, including various EMS, Fire, Police and County response agencies will test their skills in a mock bombing scenario at Rockland Community College. Tested objectives include interagency communications, trauma care and unified incident command.
Source: http://www.co.rockland.ny.us/Fire/press/06−24−05.htm

[Return to top]

Information Technology and Telecommunications Sector

22. *June 24, Storage Pipeline* — **Shareholders approve Symantec−Veritas merger.** Shareholders of Symantec Corp. and Veritas Software Corp. overwhemingly approved the merger of the two companies Friday, June 24, at special meetings of their respective stockholders. The merger is expected to close on July 2. Separately, Symantec stockholders approved an increase in the authorized number of shares of Symantec common stock to 3 billion shares.
Source: http://www.storagepipeline.com/showArticle.jhtml?articleID=1 64902639

23. *June 24, Security Focus* — **Sun Solaris traceroute multiple local buffer overflow vulnerabilities.** Sun Solaris traceroute is affected by multiple local buffer overflow vulnerabilities. These vulnerabilities present themselves when the application handles excessive data supplied through command line arguments. These issue are reported to affect /usr/sbin/traceroute running on Sun Solaris 10. Some reports indicate that this issue cannot be reproduced. It is also reported that this issue is only exploitable on the Solaris x86 platform.
Source: http://www.securityfocus.com/bid/14049/info

24. *June 24, Security Focus* — **IBM DB2 Universal Database unspecified authorization bypass vulnerability.** IBM DB2 Universal Database is susceptible to an authorization bypass vulnerability. This issue is due to a failure of the application to properly enforce authorization restrictions for database users. Users with SELECT privileges on in a database may bypass authorization checks to execute INSERT, UPDATE, or DELETE statements. Further details are not available at this time. This BID will be updated as more information is disclosed. This

vulnerability allows attackers to modify or destroy data without having proper authorization to do so. IBM has released an advisory, along with fixes to address this issue.
Source: http://www.securityfocus.com/bid/14057/info

25. *June 24, vnunet.com* — **Spoofing flaw hits major browsers.** Security company Secunia has warned of a flaw in a number of browsers that could expose users to phishing attacks. The company claims that most major browsers, including Internet Explorer, Firefox and Safari, suffer from a so−called Dialog Origin Spoofing Vulnerability. Opera 8.01 is not affected by the flaw. A hacker could use a JavaScript dialog box to request a web visitor to enter confidential information. The flaw centers around the fact that users have no way of verifying the origin of the dialog box. Hackers could exploit the flaw by offering a link to a trusted Website that simultaneously provides a malicious pop up that asks for confidential information. Microsoft has acknowledged the threat, but said that it will not release a patch because it uses a "current standard web browser functionality." Instead the software vendor urged users to use common sense before entering confidential information through a Web browser. "If a particular window or dialog box does not have an address bar and does not have a lock icon that can be used to verify the site's certificate, the user is not provided with enough information on which to base a valid trust decision about the window or dialog box," said Microsoft.
Source: http://www.vnunet.com/vnunet/news/2138716/spoofing−flaw−swee ps−browsers

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT reports scans for port 10000/tcp have been increasing ever since the release of the Veritas Backup Exec exploit. This exploit is now available in various easy to use forms, including a Metasploit plug−in. For more information, please see http://www.us−cert.gov/current/current_activity.html *UPDATE: Further reports of increased activity on port 6101. Review of the information available revealed a large spike in port 6101 connection attempts. The spike seemed to be comprised of as many new source IPs as previously seen source IPs. Activity targeting TCP port 10000 has significantly increased since the release of the Metasploit Framework module. Administrators are strongly urged to apply the hotfixes as soon as possible. Strict filtering of TCP port 10000 and 6101 is also highly recommended. For specific hotfixes and udpates please review the following URLs: * http://seer.support.veritas.com/docs/276604.htm * http://www.metasploit.org/projects/Framework/modules/exploits/backupexec_agent.pm

Current Port Attacks

Top 10 Target Ports	135 (epmap), 445 (microsoft−ds), 27015 (halflife), 1026 (−−−), 6881 (bittorrent), 139 (netbios−ssn), 4672 (eMule),

	50000 (SubSARI), 137 (netbios−ns), 53 (domain) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

26. *June 27, ABC7 (IL)* — **Chicago pairing surveillance cameras with gunshot recognition systems.** Chicago officials are using new technology that recognizes the sound of a gunshot within a two−block radius, pinpoints the source, turns a surveillance camera toward the shooter and places a 911 call. Officials can then track the shooter and dispatch officers to the scene. "Instead of just having eyes, you have the advantage of both eyes and ears," said Bryan Baker, chief executive officer of Safety Dynamics in Oak Brook, which makes the systems. After a successful pilot program, Chicago officials have installed 30 of the devices alongside video surveillance cameras in high−crime neighborhoods, with 12 more on the way, and dozens more to follow, Baker said. The system's formal name is Smart Sensor Enabled Neural Threat Recognition and Identification −− or SENTRI. And the technology is not just gaining favor in Chicago. In Los Angeles County, the sheriff's department plans to deploy 20 units in a pilot test, and officials in Tijuana, Mexico, recently bought 353 units, Baker said. Police in Philadelphia and San Francisco are close to launching test programs of their own, and New Orleans and Atlanta have also made inquiries.
Source: http://abclocal.go.com/wls/news/062605_ap_ns_gunshot−recog.h tml

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures:

DHS/IAIP Daily Open Source Infrastructure Reports − The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS/IAIP Daily Open Source Infrastructure Report is available on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

Homeland Security Advisories and Information Bulletins − DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact. Homeland Security Advisories and Information Bulletins are available on the Department of Homeland Security Website: http://www.dhs.gov/dhspublic/display?theme=70

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

DHS/IAIP Disclaimer